ABSTRACT OF THE DISCLOSURE

The random numbers are generated so as to perform an encryption processing and an authentication processing, thereby accomplishing an in-advance computation and a parallel computation. Also, the encryption processing and the authentication processing are performed, using the generated random numbers whose length is shorter than 2N with reference to the message length N. Concretely, the random numbers are generated using a pseudo random-number generator, and the generated random numbers are divided on each block basis. Also, a plaintext is divided on each block basis as well. Next, the exclusive-OR logical sums of random-number blocks R_i ($1 \leq i \leq N+1$) and plaintext blocks P_i ($1 \leq i \leq N$) are figured out, thereby acquiring ciphertext blocks C_i ($1 \leq i \leq N+2$). Moreover, a hash function performs a key-accompanying input of the random-number blocks R_i ($1 \leq i \leq N+1$), thereby generating the message authentication code of the generated ciphertext.